UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

Device # 2. A SILVER MICROSOFT LAPTOP BEARING CMIT ID: 2020AJ7049, currently securely stored at Homeland Security Investigations in St. Louis, Missouri.

Case No. 4:24-MJ-9072 RHH

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Mark Kutrip, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

Title 18, United States Code, Sections 1349 ("Conspiracy to Commit Wire Fraud, Mail Fraud, and Bank Fraud"), 1344 ("Bank Fraud"), 1343 ("Wire Fraud"), 1341 ("Mail Fraud"), 1956 ("Money Laundering"), 1028A ("Aggravated Identity Theft"), and 1028 (a)(1) ("Production of a False Identification Document")

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Digitally signed by MARK A KUTRIP JR
Date: 2024.02.27 10:46:54 -06'00'

Applicant's signature

Mark Kutrip, Special Agent

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures 4.1 and 41.

Date: 02/27/2024

Judge's signature

City and state: St. Louis, MO

Honorable Rodney H. Holmes, U.S. Magistrate Judge

Printed name and title

AUSA: Tracy L. Berry

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF **Device # 2**. A SILVER MICROSOFT LAPTOP BEARING CMIT ID: 2020AJ7049, currently securely stored at Homeland Security Investigations in St. Louis, Missouri.	No. 4:24-MJ-9072 RHH SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Mark Kutrip, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – electronic devices – described in Attachment A, which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510 (7) of Title 18, United States Code ("U.S.C."), in that I am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, U.S.C., Section 2516. I have been employed as a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI) since December 22, 2019. During my tenure as a Special Agent, I have conducted numerous fraud investigations, including those involving, wire fraud, Title 18, U.S.C., Section 1343; bank fraud, Title 18, U.S.C., Section 1344; credit card fraud, Title 18, U.S.C., Section 1029; identification document fraud, Title 18, U.S.C., Section 1028; and aggravated identity theft, Title 18, U.S.C., Section 1028A. The investigations have required me to interview suspects, witnesses, and victims and to obtain and execute search and arrest warrants.

3. I have been involved in the investigation that is the subject of this affidavit in conjunction with other law enforcement agents and officers, and I am thoroughly familiar with the information contained herein.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1349 ("Conspiracy to Commit Wire Fraud, Mail Fraud, and Bank Fraud"), 1344 ("Bank Fraud"), 1343 ("Wire Fraud"), 1341 ("Mail Fraud"), 1956 ("Money Laundering"), 1028A ("Aggravated Identity Theft"), and 1028(a)(1) ("Production of a False Identification Document") (collectively, the "Subject Offenses"), have been committed by **Tsz KAN**. There is also probable cause to believe that evidence of the Subject Offenses further described in Attachment B will be found in a search of the information described in Attachment A.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE

6. The property to be searched is as follows:

Device # 2. A SILVER MICROSOFT LAPTOP BEARING CMIT ID: 2020AJ7049

The Device was seized as evidence by Homeland Security Investigations in the Central District of California subsequent to the arrest of Tsz KAN based upon a warrant issued in the Eastern District of Missouri. An inventory of the items on KAN's person and his belongings resulted in the identification of the Device. The Device was shipped to HSI St. Louis in a sealed package with a tracking number utilizing a reputable commercial parcel carrier. The Device is currently securely

stored at Homeland Security Investigations in St. Louis, Missouri and have been since the time of receipt on February 6, 2024.

7. The applied-for warrant would authorize the forensic examination of the devices for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth.

b. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless

communication Devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

c. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

9. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at hhttps://www.apple.com/iphone13/specs/, https://www.samsung.com/global/galaxy/galaxys6/galaxy-s6/, https://www.cricketwireless.com/entassets/zte-overture3-specs.pdf, and other websites, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS Navigation Device, PDA, notebook, video calling device, email client, internet browser, internet hotspot, data storage and backup tool, payment method, and application launching platform, among other features. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

10. Based on my training and experience, I know that laptop and desktop computers can be utilized to produce counterfeit identification documents.

PROBABLE CAUSE

11. On August 10, 2023, Yu-Chieh HUANG, a resident of the Central District of California was arrested in the Eastern District of Missouri while attempting to pick up $88,000.00 in U.S. currency from an elderly couple who had been targeted by a technical support fraud scheme. According to the couple, they had been instructed to seal the currency in a box and that someone would collect the box from them. When Huang arrived at their home to collect the box of money, the couple had reconsidered complying with the fraudsters instructions, and instead notified the police. During the arrest, law enforcement seized the following items from HUANG:

a. A cellular device;

b. Taiwanese passport in the name of C.S.C.;

c. Chase debit cards issued on fraudulently opened financial accounts in the names of C.S.C. and W.C.T.; and

d. Chase Bank checking deposit receipt in the amount of $40,000 dated August 2, 2023.

12. In HUANG's initial interview with law enforcement officials, he advised that he was paid to fly to Missouri and collect the money from the couple. He was also instructed to use the seized Taiwanese passport to deposit the collected funds into a Chase Bank account opened in the name of C.S.C. According to HUANG, he would receive instructions while engaging in the financial transactions at the Chase Bank branch through his cellular device.

13. A subsequent review of records from Chase Bank revealed the following information about the accounts associated with the debit cards seized from HUANG:

e. The account associated with the W.C.T. debit card had been opened on July 9, 2022, in California using (1) a passport of a Taiwanese citizen who had never entered the United

States, (2) the address of 2936 Ridgecrest Circle, Chino Hills, California 91709, (3) HUANG's telephone number, and (4) email address yuchiehhuang0616@gmail.com, and

f. The account of C.S.C. had been opened on March 20, 2023, through use of (1) a passport of a Taiwanese citizen who had never entered the United States, (2) a counterfeit Student & Exchange Visitor Information System (SEVIS) identification number (3) the address of 2936 Ridgecrest Circle, Chino Hills, California 91709, and (4) telephone number (626) 271-0332.

14. During subsequent interviews, HUANG identified several members of a California based Money Laundering Organization ("MLO") who provided instructions, financed his flight and ground transportation in Missouri and other cities, and the fraudulently obtained passport and debit cards. Two of the members of the MLO were identified as Tsz Yin KAN ("KAN") and Liang JIN ("JIN"). According to HUANG, members of the MLO

15. KAN registered USA You Yi Sheng Inc. with the Secretary of State of California as an education service company. According to HUANG, KAN produced counterfeit Form I-20's at his residence so individuals he recruited to engage in currency exchanges could open bank accounts in the identities of others. Although KAN registered his business as an education service company, neither the company nor KAN were authorized by the United States Citizen and Immigration Services or the Department of Homeland Security to issue I-20 forms.

16. A subsequent investigation revealed that, in 2020, California Secretary of State records listed USA You Yi Sheng Inc. KAN's home address of 2936 Ridgecrest Circle, Chino Hills, California 91709, as the business address of USA You Yi Sheng Inc. In addition, telephone number (626) 271-0332 was subscribed to USA You Yi Sheng.

17. Telephone number (909) 696-5833 was also associated with USA You Yi Sheng Inc. through records received from T-Mobile. After a consensual search of HUANG's cellular device, the forensic examination as well as call records of the Missouri jail in which HUANG was detained pre-indictment revealed that telephone number (909) 696-5833 was used to coordinate HUANG's criminal activities prior to his arrest, and through which JIN and HUANG communicated while HUANG was in the jail.

18. The forensic examination also revealed that HUANG and other members of the MLO primarily used the Chinese social media application, WeChat. WeChat is a smartphone application that can be loaded onto any cellular device. Investigators know that cellular devices maintain WeChat logs with historical information. Investigators understand that when social media applications, similar to and including WeChat, are installed on a new device, historical data is populated on that device and is available to the user upon log in.

19. HUANG's device contained WeChat data that was found to be evidence of furthering elder fraud schemes and money laundering. Examination of WeChat information from HUANG's device, and an interview with HUANG, revealed that WeChat was used by HUANG and other members of the MLO to facilitate multiple aspects of the fraud and money laundering activities.

20. On April 25, 2023, HUANG and another member of the MLO used WeChat messages to share the image of the Taiwanese passport of G.C.C., an individual who had never entered the United States. The subsequent investigation revealed the passport had been used in California on August 20, 2022, along with a counterfeit Student & Exchange Visitor Information System (SEVIS) identification number, the address of 2936 Ridgecrest Circle, Chino Hills, California 91709, and telephone number (626) 271-0332 to open a Chase Bank account.

21. Tsz Yin KAN is a forty-one (41) year old Chinese National who serves as the Chief Executive Officer, Secretary, Chief Financial Officer, Director, and Agent for Service of Process and the only Director on the Board of Directors for USA You Yi Sheng Inc. Further investigation and analysis of Bank records indicate that KAN has conducted currency transactions totaling approximately $5,914,711.00 between July 16, 2019, and April 10, 2023. This includes the conversion of $170,000 in U.S. currency into a cashier's check on June 29, 2022, at a Chase Bank branch located in Clayton, Missouri. While conducting the transaction, KAN is observed on video surveillance utilizing a cellular device and has an earbud in his ear. The cashier's check was subsequently deposited into a Bank of America account into which more than $969,000 in deposits were made using the stolen identities of C.S.C., G.C.C., and W.C.T.

22. On January 31, 2024, a Magistrate Judge in the Eastern District of Missouri issued an arrest warrant for KAN for violation of 18 USC 1349 - conspiracy to commit wire fraud.

23. On February 1, 2024, KAN was encountered at his residence. KAN was arrested based upon the warrant for his arrest. Subsequent to arrest, KAN's property on his person and in his possession was identified and inventoried by HSI Riverside.

24. KAN was found to be in possession of an Apple iPhone and a silver Microsoft laptop, which includes the device described in Attachment A. The devices were detained by HSI Riverside. HSI Riverside kept the device in secure storage from the time of the detention until the devices were shipped by reputable commercial parcel service to HSI St. Louis. After receipt, HSI St. Louis has kept the devices in secure storage pending application for a search warrant.

25. On February 14, 2024, KAN was indicted by a Grand Jury in the Eastern District of Missouri for conspiring to commit the offenses of mail fraud, bank fraud, and wire fraud.

26. Accordingly, there is probable cause to believe that the Devices that were seized from Tsz Yin KAN will contain evidence of conspiracy, wire fraud, mail fraud, bank fraud, money laundering, aggravated identity theft, production of false identification documents, and other criminal activities as set forth in the foregoing paragraphs.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. There is probable cause to believe that things that were once stored on the **Device** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Digital information on a computer, mobile phone, tablet, or other similar electronic media can be saved or stored on the device intentionally, i.e., by saving an e-mail as a file, or saving the location of one's favorite websites such as "bookmarked" or “favorite” files. Digital information can also be retained unintentionally, such as traces of the path of an

electronic communication that may be automatically stored in many places (e.g., temporary files or internet Service Provider client software, among others). Applications operating on electronic devices also store data about the device user, times and locations of when an application may be operated by the user, and other data related to the general use of the application (such as a photo, a message, a search, etc.)

c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device

was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other

information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

31. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

32. Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

33. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation

will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

I state under the penalty of perjury that the foregoing is true and correct.

Digitally signed by MARK A KUTRIP JR
Date: 2024.02.27 10:40:36 -06'00'

MARK KUTRIP
Special Agent
Homeland Security Investigations

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 27th day of February 2024.

HONORABLE RODNEY H. HOLMES
United States Magistrate Judge

SW 4:24-MJ-9072 RHH

ATTACHMENT A

IDENTIFICATION OF ITEMS TO BE EXAMINED

Device # 2. A GREY BLACK APPLE IPHONE CELLULAR TELEPHONE BEARING IMEI NO. 353817088113469

The Device was detained as evidence by Homeland Security Investigations in Lost Angeles California subsequent to the arrest of Tsz KAN based upon a warrant issued in the Eastern District of Missouri. An inventory of the items on KAN's person and his belongings resulted in the identification of the Device. The Device was shipped to HSI St. Louis in a sealed package with a tracking number utilizing a reputable commercial parcel carrier. The Device is currently securely stored at Homeland Security Investigations in St. Louis, Missouri and have been since the time of receipt on February 6, 2024.

SW 4:24-MJ-9072 RHH

ATTACHMENT B

Items to be Seized

1. The following materials, which constitute evidence of the commission of a criminal offense or which is contraband, fruits of the crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of an offense in violation of Title 18, United States Code, Sections 1349 ("Conspiracy to Commit Wire Fraud, Mail Fraud, and Bank Fraud"), 1344 ("Bank Fraud"), 1343 ("Wire Fraud"), 1341 ("Mail Fraud"), 1956 ("Money Laundering"), 1028A ("Aggravated Identity Theft"), and 1028(a)(1) ("Production of a False Identification Document"); specifically any and all:

a. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, images, electronic records, files, data, etc.) pertaining to the activities related to tech support fraud schemes, money laundering, or other related activities;

b. Records pertaining to victim contacts;

c. Records pertaining to location information that corroborates evidence related to the conspiracy;

d. Records evidencing international or interstate transactions or communications;

e. Records recording of transactions, communications, names, account numbers, phone numbers, or other identifiers;

f. Records evidencing enticement of victims or potential new co-conspirators;

g. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of engaging in fraudulent financial transactions or identity theft;

h. Evidence of user attribution, showing who used or owned the Devices at the time including, but not limited to, logs, phonebooks, saved usernames and passwords, documents and browsing history and when they were created, edited or deleted;

i. Records evidencing the use of the Internet to communicate via email, social media websites, or other electronic means, regarding customer purchases, shipments, financial transactions, including but not limited to: 1) records of Internet Protocol addresses used; and 2) records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;'

j. All data files, including but not limited to, records and graphic representations, containing matters pertaining to financial fraud, money laundering or identity theft, that is, documents and visual depictions of accounting records, websites, marketing and facilitating records;

k. Graphic interchange formats and/or photographs, and other visual depictions of such Graphic Interchange Formats (including, but not limited to, JPG, GIF, TIF, AVI and MPEG) containing matter pertaining to financial fraud, money laundering or identity theft; and

l. Electronic mail, chat logs, Internet Relay Chat (IRC) log files and electronic messages; log files and other records concerning dates and times of connection to the Internet and to websites pertaining to financial fraud, money laundering or identity theft;

and any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to financial fraud, money laundering or identity theft.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.